

Title of Document	Data Breach Risk Management
Name of Department	Quality

What type of document is this?	Work Instruction (WI)	
Which Helping Hands policy/SOP does this WI relate to?		Index number of policy/SOP

Which Operational Priority/Priorities does this document link to?	Governance Framework	Maximising Efficiency & Cost Management	Internal & External Communications	Information Management & Technology
---	----------------------	---	------------------------------------	-------------------------------------

Custodian of document	Group Managing Director	Committee responsible for this document	Policy Committee
Approval date and committee chairperson signature	26.02.2025	When is its next scheduled review?	26.02.2028

Who does it apply to?	The Quality team to ensure clarity and guidance on process						
	Does it apply to bank workers?	Yes	Does it apply to agency staff?	Yes	Does it apply to third party contractors?	Yes	

Purpose of the Work Instruction	This working instruction is to be used in conjunction with the Helping Hands Data Breach procedures to ensure that breach detection, investigation, internal reporting and notification where applicable, takes place. This document facilitates risk assessment and notification process.
---------------------------------	--

## 1.0 RISK ASSESSMENT GRID AND SCORE RATIONALE

### 1.1 Risk Rating Key:

<b>Extreme –</b> Consultation with DPO required, DPO report to ICO, Executive team, Board and affected individuals	<b>High –</b> Notification to affected Individuals, Consultation with DPO required	<b>Moderate –</b> Notification to affected individuals, consultation with DPO on a case-by-case basis	<b>Low –</b> Notification to affected individuals
---	---	--	--

**RISK = Likelihood x Impact**



## 1.2 Risk Assessment Grid

Likelihood that individuals have been affected (harm)					
Almost Certain	Moderate	High	Extreme	Extreme	Extreme
Likely	Low	Moderate	High	Extreme	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Low	Moderate
	Negligible	Minor	Moderate	Major	Severe
	Impact (severity)				

### Step 1: Likelihood of affecting individuals

Likelihood	Description
Rare	Isolated incident. No evidence to support that harm has occurred. Not a frequent or regular occurrence. No lasting effect is anticipated
Unlikely	Isolated incident unlikely to reoccur. No evidence to support that harm has occurred. Not a frequent or regular occurrence. No lasting effect is anticipated
Possible	Potential to occur frequently and regularly and possibly affect individual
Likely	Likely to occur frequently and regularly and likely to affect individual
Almost Certain	Recurring and frequent, predictable patterns, almost certain to affect individual

## Step 2: Impact of the Breach

Severity	Description
<b>Negligible</b>	<ul style="list-style-type: none"> <li>No risk to individual rights and freedoms resulting from the breach</li> <li>Minimal effect and/or risk of harm to affected individuals.</li> <li>Data containment measures in place at time of breach*</li> <li>Minimal exposure at unsecured location</li> <li>No risk of confidential information leading to embarrassment</li> <li>No risk of litigation, ID fraud, loss of funds or employment</li> </ul>
<b>Minor</b>	<ul style="list-style-type: none"> <li>Minor risk to individual rights and freedoms resulting from the breach</li> <li>Minor effect and/or risk of harm to affect individuals</li> <li>Data containment measures in place at time of breach*</li> <li>Minimal exposure at unsecured location</li> <li>Low risk of confidential information leading to embarrassment</li> <li>Low risk of litigation, ID fraud, loss of funds or employment</li> </ul>
<b>Moderate</b>	<ul style="list-style-type: none"> <li>Due care/process below reasonable expectations in several ways, but not for prolonged periods.</li> <li>Has potential to impact on service provision and /or affects vulnerable individuals.</li> <li>Requires investigation relating to compliance and risk management issues.</li> <li>Some potential for litigation and adverse local publicity</li> </ul>
<b>Major</b>	<ul style="list-style-type: none"> <li>Due care/process below reasonable expectations in several ways which may have a lasting effect</li> <li>Likely to impact on service provision and /or affects vulnerable individuals.</li> <li>Requires investigation relating to compliance and risk management issues.</li> <li>Likely for litigation and adverse local publicity</li> </ul>
<b>Severe</b>	<ul style="list-style-type: none"> <li>Significant issues regarding standards, quality of care, and safeguarding of, or breach of rights and freedoms.</li> <li>Compliance and risk-management issues causing long term issues for those affected.</li> <li>Loss of control of personal data, unauthorised reversal of anonymization /pseudonymisation</li> <li>High probability of loss of employment, financial loss and/or fraud</li> <li>Excessive and disproportionate volume affected by breach.</li> <li>Will require immediate and in-depth investigation due to the potential risk of embarrassment and/or discrimination</li> <li>May involve serious safety issues, reputational damage and/or strong possibility of adverse national publicity.</li> <li>A high probability of litigation, financial loss, decline in health and/or death</li> </ul>

## 2.0 Data Containment Measures

There are circumstances where containment action will negate the need to notify the ICO of a breach of personal data.

- **encryption** – where the personal data is protected by means of encryption.
- **‘trusted’ partner** - where there may be a confidentiality or availability breach whereby personal data is accidentally sent or disclosed the wrong department or a regular contractor known to Helping Hands. In such situations, the data may be recovered, returned or securely destroyed. The recipient may still be considered “trusted” even if the data has been accessed if Helping Hands can be assured that the data has not been further compromised.
- **cancel the effect of a breach** - where the controller can null the effect of any personal data breach

Helping Hands acknowledges that such cases will need to be reported and risk assessed following a breach. This in turn may reduce the risk to individuals warranting a ‘near event’ classification and rendering notification to ICO unnecessary;

### 2.1 Sensitivity Factors

Certain factors need to be considered and incorporated in to the grading scores. When a breach involves special category data and/or vulnerable groups, this will increase the risk score and may lead to notification to affected individuals and ICO being a higher priority.

### 2.2 Vulnerable Groups

- Children and vulnerable young people
- Vulnerable adults with Safeguarding concerns

### 2.3 Special Categories of personal data

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person’s sex life or sexual orientation

### 2.4 Other data not listed under GDPR

- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or

individual

- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

### 3.0 Notification Procedure

Article 34 of GDPR requires that any personal data breach resulting in a high risk of harm/impact to the rights and freedoms of individuals needs to be communicated with those affected with the following notable exceptions:

**The controller (Helping Hands) has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach; for example, the data were encrypted.**

**The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.**

**It would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.**

The article outlines that a data breach with a significant risk score as indicated in the risk rating key needs to be reported to the relevant authority who are the ICO.

The following information is to be included in any notification in both circumstances and shown below:

- A description of the nature of the personal data breach, data category and approximate number of data subjects and volume of records where possible
- Name and contact details of the DPO or other contact from whom more information can be obtained
- Description of the likely consequences of the breach and
- Description of the measures taken or proposed to address the breach, including any measures to mitigate possible adverse effects.

Article 33 of GDPR requires reporting of a breach within 72 hours. This period starts when Helping Hands becomes aware of the breach and not necessarily when the breach occurred. There must be an established process to determine that a security incident has occurred which has led to personal data being compromised.

**Don't** delay in reporting an incident if you are unsure on whether to report– if in doubt err on the side of caution and **notify**.

**Don't** put anything in the report that could be considered personal confidential data (such as patients / service user details)

If the decision is made not to notify individuals, there may still be a need to notify the ICO unless Helping Hands can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel organisations to inform affected individuals if it considers there is a high risk.

There must be clear documentation of any decision-making process in line with the requirements of this SOP.

**Where the 72hour deadline is not met, an explanation must be provided to the authorities as failure to notify promptly may result in additional action by the ICO in respect to GDPR.**

### 3.1 What to expect following notification

An email from the ICO will be sent to confirm receipt of the notification and an ICO case reference number which must be noted and quoted in any further correspondence with the ICO in relation to the incident.

### 3.2 Records

All documentation, records and information pertaining to a breach must be logged, maintained and made available on request. The current location is:

- **SharePoint / Home / Record Keeping/ Data Breach Incident Log**
- **SharePoint / Documents / GDPR Compliance/ Data Breach/ DIN Forms**

The Information Commissioner will then decide if any action is necessary and whether other authorities need to be notified and to what extent.

**Note – Equality Impact Assessments are not required for Work Instructions**

What was the previous version number of this document?	Version 01	
Changes since previous version	Review of section 1.0 - Risk Management Grid and rationale. Aligned with data incident notification form.	
Who was involved in developing / reviewing/ amending this work instruction?	GDPR Co-Ordinator Data Protection Officer Quality Development Lead	
How confidential is this document?	Restricted	Can be shared freely within Helping Hands but NOT outside
Associated Documents	Data Protection Policy Data Incident Notification (DIN) Form	